Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 19:54:32 UTC

Tool: QUIETEXIT

Names	QUIETEXIT
Category	Malware
Type	Backdoor, Tunneling
Description	(Mandiant) QUIETEXIT works as if the traditional client-server roles in an SSH connection were reversed. Once the client, running on a compromised system, establishes a TCP connection to a server, it performs the SSH server role. The QUIETEXIT component running on the threat actor's infrastructure initiates the SSH connection and sends a password. Once the backdoor establishes a connection, the threat actor can use any of the options available to an SSH client, including proxying traffic via SOCKS. QUIETEXIT has no persistence mechanism; however, we have observed UNC3524 install a run command (rc) as well as hijack legitimate application-specific startup scripts to enable the backdoor to execute on system startup.
Information	<https://www.mandiant.com/resources/unc3524-eye-spy-email>
MITRE ATT&CK	<https://attack.mitre.org/software/S1084>
Malpedia	<https://malpedia.caad.fkie.fraunhofer.de/details/elf.quietexit>

Last change to this tool card: 30 November 2023

Download this tool card in JSON format

All groups using tool QUIETEXIT

Changed	Name	Country	Observed	
APT groups				
	APT 29, Cozy Bear, The Dukes		2008-Feb 2025	

1 group listed (1 APT, 0 other, 0 unknown)

Source: https://apt.etda.or.th/cgi-bin/listgroups.cgi?u=f7540533-ada8-45ac-915d-1c550090338a